



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/692,747	10/18/2000	Craig L. Ogg	39478/RRT/S850	7075
23363	7590	11/23/2005	EXAMINER	
CHRISTIE, PARKER & HALE, LLP			HEWITT II, CALVIN L	
PO BOX 7068			ART UNIT	
PASADENA, CA 91109-7068			PAPER NUMBER	

3621

DATE MAILED: 11/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/692,747

Applicant(s)

OGG ET AL.

Examiner

Calvin L. Hewitt II

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Status of Claims

1. Claims 1-45 have been examined.

Response to Amendments/Arguments

2. Applicant is of the opinion that the prior art does not teach a user registered with a first computer. The Examiner respectfully disagrees. Sudia clearly teaches that in order for a user to send an encrypted communication from a device the user must have a device certificate (column 21, lines 15-23). The certificate comprises the device serial number, the device public signature verification key and the user's public encryption key (column 18, lines 5-11), and is loaded onto the device prior to use of the device (column 21, lines 15-23). Hence, the user is registered with the device as the user is allowed to send encrypted communications using said device. Similarly, if the user was not registered with the device the user would not be able to send an encrypted message and have to obtain a certificate (column 18, lines 5-11) in order to do so (note: if the user is registered with a first computer and not a second, then the user would have to "re-register" with the second computer because the escrow center already has the user encryption key on file from the first computer registration).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-5, 7-19, 21-31, 33-30 and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia, U.S. Patent No. 6,009,177.

As per claims 1-5, 7-19, 21-31, 33-30 and 41-45, Sudia teaches a digital communications security system comprising:

- a user using one or more computers (column 1, lines 20-58; column 2, lines 55-63; column 13, lines 30-63; column 16, lines 9-34; column 21, lines 15-53)
- a secret key for identifying a first computer and registering a user
- a remote system that communicates with one or more user computers and receives user information and a secret key for registering a user (i.e. registering a user with an online system) (column/line 17/29-18/11)
- a user that uses said first computer for second and subsequent communications with the remote system (column 21, lines 15-53)

- a secret key that comprises an encrypted randomly generated hash message authentication key that is generated at the time of registration (column/line 17/50-18/11; column 25, lines 27-51)
- a secret key that comprises an encrypted randomly generated hash message authentication key for digitally signing electronic communications thereby authenticating the user, storing said key at the user computer and changing said key at periodic intervals (column 15, lines 45-58; column 17, lines 37-48 and 55-64; column 21, lines 40-54; column 41, lines 15-43)

Applicant has amended the claims 1, 16 and 29 to include the language of a re-registration wizard for requiring a user to re-register if a second computer used to access the system is physically different than a first registered computer. Sudia teaches a user computer sending an encrypted secret key to the remote system that decrypts and stores the secret key (column/line 17/50-18/11) as part of a method for receiving an escrow certificate. Sudia specifically requires a user to possess a valid escrow certificate in order to access the system (e.g. encrypt and decrypt communications) (column 21, lines 15-20 and 27-40). Therefore, Sudia teaches Applicant's "re-registration" wizard if a user tries to access the system using a second computer that lacks a valid certificate and is different from

a recently registered computer that has obtained such a certificate (column 17, lines 29-49; column/line 22/63-23/12).

Sudia does not explicitly recite the type of keys used by the remote system to perform such a function. However, as Sudia recites symmetric key encryption (shared key), encryption using session keys, asymmetric encryption (public/private or secret keys used for decryption/encryption or encryption/decryption), the specific methods of Diffie-Hellman, RSA, Micali, DES, etc. It would have been at least obvious for one of ordinary skill to choose any of the disclosed methods by Sudia to enable to parties to communicate cryptographically.

Limitations identifying the type of VBI used or system with which a user is registering is merely non-functional descriptive material and, non-functional descriptive material cannot render non-obvious an invention that would have been otherwise been obvious (In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983).

Regarding postal security devices, the teachings of Sudia are broadly applied to trusted devices that comprise an embedded microprocessor, input-output interface, memory and optionally a cryptographic co-processor (column 13, lines 30-63). A PSD is an element of the set of "trusted devices" as it comprises the features identified above. In addition, PSD's print "value bearing

instruments" (VBI). Therefore, it would have been obvious to one of ordinary skill to apply the teachings of Sudia to trusted devices such as PSDs.

Sudia does not explicitly recite user computers communicating with a system that is a server system. However, Sudia teaches a user first computer communicating with another user computer (column 21, lines 27-29), securing digital communications (column 2, lines 55-63) and distributed data processing systems such as those used for distributing electronic mail (column 1, lines 20-40), hence, it is at least obvious to one of ordinary skill for the user computer to communicate with the escrow agent computer system (i.e. remote system) over computer network (figures 15 and 16) such as the internet.

5. Claims 6, 20, 32, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia, U.S. Patent No. 6,009,177 in view of Ote et al., U.S. Patent No. 6,023,506.

As per claims 6, 20, 32, and 40, Sudia teaches a digital communications security system that uses encryption keys for encrypted user computer specific information such as a secret key comprising an encrypted randomly generated hash message authentication key that is generated at the time of registration (column/line 17/50-18/11; column 25, lines 27-51). However, Sudia does not explicitly recite a specific encryption method for encrypting the user computer specific information. Ote et al. teach a method for generating an encryption key

using a user pass-phrase (abstract). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Sudia and Ote et al. in order to reduce the burden on users regarding the management of encrypting information ('506, column/line 1/65-2/6).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Art Unit: 3621

7. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, James P. Trammell, can be reached at (571) 272-6712.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

c/o Technology Center 2100

Washington, D.C. 20231

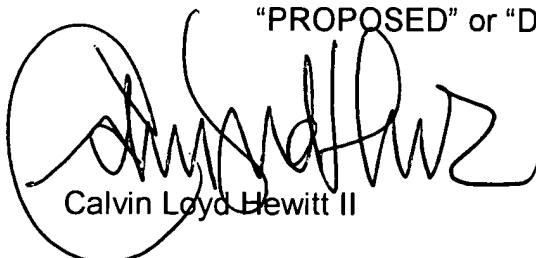
or faxed to:

(571) 273-8300 (for formal communications intended for entry and after-final communications),

or:

(571) 273-6709 (for informal or draft communications, please label

"PROPOSED" or "DRAFT")

A handwritten signature in black ink, appearing to read 'Calvin Hewitt II', is written over a circular stamp. The signature is fluid and cursive.

Calvin Loyd Hewitt II

November 21, 2005